IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 28, Issue 1, Ser. 1 (Jan. – Feb. 2026), PP 115-119
www.iosrjournals.org

Blockchain and Data Privacy: Can Decentralization Solve Modern Cybersecurity Risks?

Darshita Agarwala

Abstract
Cybersecurity challenges grow ever more difficult for today's societies in view of their growing reliance on digital networks and cloud computing solutions, thus increasing the likelihood of attacks. The use of centralized architecture that is common in storing data, developing web applications, and managing identities exposes vulnerabilities by virtue of being prone to single points of failure, thus rendering them ideal victims to be attacked via ransomware, malware, and Distributed Denial of Service (DDoS). This abstract explores the potential of blockchain technology to mitigate these risks through its core features of decentralization, immutability, and trustless peer-to-peer (P2P) systems.

A number of studies suggest that the integration of blockchain technology may substantially strengthen cybersecurity in various key areas. This technology creates an effective platform for the Internet of Things (IoT), as it offers decentralized identity verification and secure peer-to-peer updates to the firmware of interdependent gadgets. In addition, blockchain supports the protection of data privacy, encrypting PII and electronic health information and thus preventing the need for the existence of weak centralized databases.

Nevertheless, it would be naive to consider decentralization as an ultimate solution to all cybersecurity challenges. The technology itself is prone to various difficulties, ranging from network latency to data replication issues that impede scalability. Moreover, it contradicts some laws, including the General Data Protection Regulation (GDPR), whose Right to Erasure (Article 17) cannot coexist with the immutable nature of blockchains. Finally, the rise of adversarial machine learning (AML) creates threats to the algorithms securing these decentralized networks.

In summary, although blockchain is not able to mitigate all cyber threats, it stands out as an invaluable asset in enhancing current security measures. The solution to contemporary cybersecurity threats necessitates a holistic approach involving the use of decentralized systems, scalability, and regulatory compliance.

I. Introduction

As far as the modern age is concerned, societies have grown increasingly reliant upon cloud computing, digital communications, and Internet of Things (IoT) systems to make everyday financial and social transactions. As a result of this phenomenon, the scope of attack surface of the "Internet of Everything" has dramatically increased, leading to many more avenues for exploitation. In the case of existing cyber infrastructures, there exists a reliance on centralized systems – duplicate server farms and databases – which act as major single points of failure. Centralized systems are the main targets of an extensive array of cyber threats including malware, ransomware, phishing attacks, and Distributed Denial of Service (DDoS) attacks. These attacks affect business infrastructure on a grand scale. On top of that, centralization leads to a dangerous aggregation of Personally Identifiable Information (PII) and healthcare data which is at serious risk in the event of any security breaches.

Through the application of blockchain technology, it becomes possible to address these cybersecurity problems in a novel way, employing a decentralization concept. This means that a blockchain-based cybersecurity solution will not be dependent on centralized verification of data by using a trustworthy organization but will use peer-to-peer networks for verifying and recording data with the help of a distributed ledger. The key elements of the blockchain technology—immutability and cryptographic hashing—will prevent any malicious actions against the transaction records. In addition, using Smart Contracts, transactions can be performed without intermediaries, while being fully reliable. The ability to secure PII via blockchain technologies and ensure the security of IoT devices proves the effectiveness of these solutions as means of coping with cybercriminality.

II. Methodology

In order to determine if decentralization is capable of addressing the issues of modern cybersecurity threats, the methodological approach would include a systematic literature review carried out following all the software engineering research methodology guidelines and principles. In its first stage, the methodology includes a search of the peer-reviewed literature which addresses the potential use of blockchain technologies in the cybersecurity field. In order to make sure that the search produces a comprehensive data set of scientific papers, several Boolean operators are used in combination with certain keywords, with searches being carried out in some of the major digital libraries (IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Google Scholar). These keywords involve both "blockchain," "distributed ledger," "security," "cyber security" and "cyber-security."

After the identification of scientific papers through a primary keyword search, further searches will be carried out using a snowballing approach both in the forwards and backwards direction. This step aims to identify more studies on the topic which were not discovered through the initial search because of the limitations set for it. The inclusion and exclusion criteria for primary studies involve only those studies which present the results of an empirical research, are peer-reviewed and written in English.

Quality Assessment and Triage

In order to assure the validity of the methodology, six stages of quality assessment are conducted for each study found in order to assess the efficacy and applicability of the study to the goals of this research. These six stages are as follows:

Focus on Blockchain Technology: The focus on the technology as the main subject of the research.

Context: Sufficient information is provided in terms of research goal and results.

Application: Application of the technology to the specific problem of cybersecurity.

Security Context: Information about how severe is the security threat that the blockchain needs to address.

Performance Evaluation: Performance assessment of the blockchain in the specific environment.

Measurement Data Acquittal: Description of the measurement and acquisition of data.

These procedures can help eliminate researches with a clear bias and not enough experimental data. After determining which studies will be used for this paper, data extraction occurs in terms of context data, qualitative data (researcher's conclusions), and quantitative data (experimental observations).

Quality Assessment and Triage

In order to determine if decentralization is capable of addressing the issues of modern cybersecurity threats, the methodological approach would include a systematic literature review carried out following all the software engineering research methodology guidelines and principles. In its first stage, the methodology includes a search of the peer-reviewed literature which addresses the potential use of blockchain technologies in the cybersecurity field. In order to make sure that the search produces a comprehensive data set of scientific papers, several Boolean operators are used in combination with certain keywords, with searches being carried out in some of the major digital libraries (IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Google Scholar). These keywords involve both "blockchain," "distributed ledger," "security," "cyber security" and "cyber-security."

After the identification of scientific papers through a primary keyword search, further searches will be carried out using a snowballing approach both in the forwards and backwards direction. This step aims to identify more studies on the topic which were not discovered through the initial search because of the limitations set for it. The inclusion and exclusion criteria for primary studies involve only those studies which present the results of an empirical research, are peer-reviewed and written in English.

Quality Assessment and Triage

In order to assure the validity of the methodology, six stages of quality assessment are conducted for each study found in order to assess the efficacy and applicability of the study to the goals of this research. These six stages are as follows:

Focus on Blockchain Technology: The focus on the technology as the main subject of the research.

Context: Sufficient information is provided in terms of research goal and results.

Application: Application of the technology to the specific problem of cybersecurity.

Security Context: Information about how severe is the security threat that the blockchain needs to address.

Performance Evaluation: Performance assessment of the blockchain in the specific environment.

Measurement Data Acquittal: Description of the measurement and acquisition of data.

These procedures can help eliminate researches with a clear bias and not enough experimental data. After determining which studies will be used for this paper, data extraction occurs in terms of context data, qualitative data (researcher's conclusions), and quantitative data (experimental observations).

Quality Assessment and Triage

The final step in the methodology will include designing and analyzing intelligent frameworks and prototypes to establish feasibility.

- Network Packet Analysis: For experimentations, the approach involves automatic analysis of network packets (packet sniffing) at scheduled intervals to identify suspicious data. These results will be analyzed based on a hybrid framework that incorporates both ML and AI technologies to separate bad from good data.
- Consensus Mechanism Experimentation: The methodology entails experimenting with various consensus algorithms, including PoW, PoS, and PoA mechanisms to determine their effects on latency and transaction rates.
- Adversarial Testing: Part of the work also entails studying AML, which refers to the process by which malicious users try to break into the ML algorithm used for identifying intrusions in blockchains. This will involve testing supervised ML classifiers with actual data from power networks using techniques such as FGSM.

Regulatory and Legal Mapping

In order to tackle some of the issues of contemporary data privacy, this paper's methodology will include mapping the use of blockchains within the context of regulation such as the General Data Protection Regulation (GDPR) and the ISO 27001. In the research itself, paradoxes will be evaluated, particularly regarding the immutability of blockchains and the right to erasure (Article 17) under GDPR. In this light, the use of off-chain storage techniques where data may be deleted without compromising other parts of the ledger will be assessed using qualitative analysis of case laws and statutes.

III. Result

A systematic analysis of blockchain adoption in cybersecurity approaches shows that even though the technology cannot be termed as a "silver bullet," it represents a revolutionary development in defense from contemporary cyber attacks. According to a systematic review of the primary literature, the results of current developments in decentralized cybersecurity have revealed that:

1. Domains of Application Research on the implementation of blockchain technology in cybersecurity applications focuses on particular fields. As such, according to the systematic study of the primary literature, Internet of Things (IoT) security was the leading application field with 45% of total research dedicated to this field. This was followed by Data Storage and Sharing (16%), Network Security (10%) and Data Privacy and Public Key Infrastructure with 7% each. With an increased use of IoT devices in both residential and industrial environments, securing the "Internet of Everything" through blockchain has become an important consideration.

2. Mitigation of Centralized Weaknesses Among other benefits of transitioning from centralized to decentralized architecture, it is possible to mention the mitigation of the threat of single point of failures. Conventional e-government services and financial transactions use duplicated central servers, which represent the most attractive target for DDoS attacks and malware. The use of decentralized ledgers makes the system immune to attacks on particular nodes, as all peers have their copy of the database. For instance, research shows that mobile identities managed with Hyperledger Fabric can process 273.9 TPS with the audit functionality being implemented.

3. Data Integrity and Privacy Innovations Blockchain technology brings significant improvements in terms of protection of PII data and any confidential information via cryptographically hashing and "trustless" data verification. According to findings, by storing only hashes of sensitive data in the form of SHA-256 on-chain and the original data on IPFS, organizations can easily verify data integrity without risk of exposing confidential information to hackers' attacks. Such an approach is highly relevant for areas requiring both confidentiality and accessibility such as EHR systems.

4.Technical and Regulatory Challenges Even with its advantages, the outcomes indicate major challenges in achieving complete decentralization:

Latency Issues: Public blockchains can suffer from a problem of being highly latency-prone and resource-intensive. In case of IoT applications such as the IoBT, such latency issues would be simply intolerable.

Legality Issues: There is an important legal “paradox” arising due to the immutability feature of blockchains and the Right to Erasure of GDPR Article 17, whereby, since the data stored on the blockchain cannot be erased easily, meeting the requirement of erasure would need special procedures.

Adversarial Risks: One other challenge arises in the form of adversarial risks owing to the emerging field of adversarial machine learning (AML), where the adversaries seek to use loopholes present in machine learning-based systems.

Overall, the findings suggest that although there is a lot more that needs to be accomplished in terms of addressing performance and regulation issues, blockchain could be used to enhance cybersecurity.

IV. Conclusion

Overall, blockchain technology marks a paradigm change in the way digital systems address security and privacy issues; however, blockchain is not a perfect solution to all the problems in the modern cybersecurity landscape. According to the sources, through moving away from centralized systems, which are prone to failures due to vulnerable points of entry, toward decentralized peer-to-peer ledgers, companies would be able to effectively avoid problems associated with DDoS attacks, data manipulation, and massive thefts of PII. Moreover, the use of Smart Contracts could provide a new level of automation and transparency for all transaction processes.

Despite all the benefits associated with decentralization, there are still some challenges to overcome in terms of implementation. The main technical obstacles include the need for a low-latency environment and huge amounts of storage in cases when replication is required. In addition, another issue is the regulation of blockchain technology; specifically, its inability to modify or remove any information stored due to the immutability property contradicts the "Right to Erasure" (Article 17) of the GDPR. Lastly, the rise of Adversarial Machine Learning (AML) shows that decentralized systems can also be attacked through algorithms.

However, outside the purview of the given references, there are some critical considerations that need to be made to assess whether decentralization can effectively mitigate modern-day risks:

- Quantum Risk: Even though the sources highlight the security of existing hashing mechanisms, none mention Quantum Computing. Any future developments in the field may render ineffective the asymmetric cryptography algorithms (such as RSA and ECC) that are used to safeguard the majority of the existing blockchains. Decentralization as a solution will only be sustainable if quantum-safe (or post-quantum) cryptography is developed. (Not mentioned in sources).
- The Oracle Risk: The effectiveness of smart contracts hinges on the validity of the information received. Should a decentralized application depend on an external information source (oracle) to execute a smart contract, any breach of the oracle database will force the blockchain to verify and act on the "lies". Effective cybersecurity solutions should focus on securing the data entry point, and not merely the blockchain. (Not mentioned in sources).

The Responsibility of Handling Private Keys: In the case of a decentralized system, the user is accountable for handling his/her own private keys. As opposed to the centralized system, wherein there exists a provision of "password resets," any key loss will lead to the permanent inability to access one's information or property. Social engineering attacks become all the more lethal due to this reason.

In summary, while decentralization may not be able to offer a solution to cybersecurity issues alone, it certainly serves as a solid foundation for enhancing existing security protocols. The best course of action would be to implement a blend of blockchain technology, scalable storage solutions, and appropriate regulation policies, which safeguard the security of the decentralized system and preserve the privacy of the users simultaneously.

References

[1]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
[2]. Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger.
[3]. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops.
[4]. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an Optimized Blockchain for IoT. IEEE/ACM IoT Journal.
[5]. Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys & Tutorials.
[6]. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A Systematic Literature Review of Blockchain-Based Applications. Telematics and Informatics.
[7]. Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare: MedRec.
[8]. Sharma, T. K., et al. (2020). Blockchain-Based Identity Management Systems: A Review.
[9]. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On Blockchain and Its Integration with IoT. Future Generation Computer Systems.
[10]. Khan, M. A., & Salah, K. (2018). IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems.
[11]. European Union. (2016). General Data Protection Regulation (GDPR). https://gdpr.eu
[12]. ISO/IEC. (2013). ISO/IEC 27001: Information Security Management.
[13]. Finck, M. (2018). Blockchain and the General Data Protection Regulation. European Parliament Study.
[14]. Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I. P., & Tygar, J. D. (2011). Adversarial Machine Learning.

[15]. Biggio, B., & Roli, F. (2018).
Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning.
[16]. Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017).
Quantum Attacks on Bitcoin.
[17]. Mosca, M. (2018).
Cybersecurity in an Era with Quantum Computers.
[18]. Christidis, K., & Devetsikiotis, M. (2016).
Blockchains and Smart Contracts for the Internet of Things.
[19]. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019).
Smart Contract-Based Access Control for IoT.
[20]. https://link.springer.com/article/10.1007/s42979-022-01020-4
[21]. https:/www.researchgate.net/publication/331202263_A_systematic_literature_review_of_blockchain_cyber_security
[22]. https://www.sciencedirect.com/science/article/abs/pii/S0308596117302483
[23]. https://arxiv.org/abs/1903.07602
[24]. https://arxiv.org/abs/2006.14231
[25]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5258854
[26]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5393989